EXHIBIT A

Cisco Systems

Cisco Compatible Extensions

Cisco Compatible Extensions Program Brochure

This document describes the Cisco® Compatible Extensions program and its benefits. The document also lists the main features of the first two versions of the Cisco Compatible Extensions specification.

Challenge

The WLAN market has grown exponentially as more users demand mobility in and out of the office. Numerous client devices have been introduced to meet the challenges of device mobility; these devices must interoperate securely with leading WLAN infrastructures and must consistently provide the features that organizations require.

Solution

With the Cisco Compatible Extensions program, WLAN client suppliers (the program's participants) license, at no charge, Cisco WLAN technology innovations in a specification. Participants implement all elements of the specification and undergo extensive testing at an independent third-party test lab. The testing helps to ensure support for innovative features pioneered by Cisco Systems, as well as interoperability with Cisco WLAN infrastructure products.

Look for the Cisco Compatible Logo

The Cisco Compatible Extensions program helps to ensure that client devices from a variety of suppliers can leverage Cisco-based WLANs. To make it easy to find these devices, Cisco has licensed the Cisco Compatible logo (Figure 1) for use by participants whose products pass all tests at the independent third-party test lab. Locating approved wireless devices is as easy as looking for the logo. Review a complete listing of products that have earned the Cisco Compatible designation.

Figure 1 - The Cisco Compatible Logo

Cisco Compatible

The Cisco Compatible logo has recently changed. For a limited time, the former logo will also be seen on products and collateral. The features and benefits of the program remain the same-only the logo has changed.

Cisco Compatible Continued Development

Through the Cisco Compatible Extensions program, Cisco shows its commitment to leading innovation and providing pre-standard features to fulfill customer requirements. Cisco enables its partners to provide software upgrades for Cisco Compatible mobile devices to ensure that there is a migration path to future industry standards and to Cisco Aironet® infrastructure features. Migration from different versions of the Cisco Compatible Extensions program is simply and easily implemented. Cisco will continue to develop future Cisco Compatible features and work with industry-leading partners to empower customers with mobility solutions to solve business challenges, today and in the future.

WLAN Adapters and Client Devices

The Cisco Compatible Extensions program for WLAN devices helps to proliferate WLAN innovations to many different WLAN client adapter form factors and client devices while maintaining interoperability.

Intel, a strategic alliance partner and lead collaborator, has achieved Cisco Compatible status for its Centrino™ Mobile technology, which is available in many notebook computers. Major notebook suppliers, including Acer, Dell, Fujitsu, IBM, HP, and Toshiba, provide Cisco Compatible notebooks.

Cisco is working closely with suppliers of mobile computing devices, such as PDAs, that have less processing power than notebooks and run fewer applications. Such devices are classified as application-specific devices (ASDs). The requirements for Cisco Compatible ASDs are a subset of the requirements for Cisco Compatible notebooks, described in the next section.

Accelerating the Availability of Innovative Features

The primary features of Cisco Compatible Version 1 are:

- Support for the Cisco Extensible Authentication Protocol (LEAP) 802.1X authentication type
- The ability to interoperate with an access point that supports multiple Service Set Identifiers (SSIDs) tied to multiple VLANs, providing benefits such as flexible security schemes in a mixed client environment

- IEEE 802.11 and Wi-Fi compliance

Cisco Compatible Version 2 provides enhanced features, including Wi-Fi Protected Access (WPA), with increased security options, quality of service (QoS), and ground-breaking RF management capabilities. These features combine to extend the Cisco Wireless Security Suite, add robustness and resiliency for highly used wireless networks, and enable Cisco Compatible clients to participate in RF management functions like interference detection, rogue access point detection, and assisted site survey.

Table 1 - Features of the Cisco Compatible Extensions Program

	Version 1.0	Version 2.0	Version 3.0
Standards	Wired Equivalent Privacy (WEP) IEEE 802.11 and 802.1X Wi-Fi compliance Windows Hardware Quality Labs (WHQL)	WPA compliance	WHQL or WI-FI (Windows) WPA & WPA2 Advanced encryption
Security	LEAP Cisco pre-standard Temporal Key Integrity Protocol (TKIP)	Protected EAP with Generic Token Card support (PEAP-GTC) Standard (WPA) TKIP with LEAP and PEAP-GTC	CCKM with EAP-FAST (migration path for LEAP users) AES provides 256-bit encryption based on 802.11 TGi
VLANs and QoS	Interoperability with access points that support multiple SSIDs and VLANs	Pre-standard enhanced Distributed Coordination Function (eDCF)	WME provides standards based QoS based on 802.11 TGi WiFi Qos WMM (Wi-Fi Multi-Media)
Performance and management		Access point assisted roaming Fast 802.1X reauthentication Radio environment reporting Access point specified maximum transmit power Cisco Compatible version control	Cisco Compatible version control Single Sign-on Proxy ARP

The following attributes are deemed optional for ASDs:

Cisco Compatible Version 1:

- Wi-Fi compliance
- Microsoft Windows Networking IEEE 802.11 NIC compatibility
- EAP-Transport Layer Security (TLS) or EAP-Message Digest Algorithm 5 (MD5) Windows XP support
- Cisco TKIP (CKIP) support
- Support for multiple SSIDs

Cisco Compatible Version 2:

- PEAP support
- WPA support

Cisco Compatible Version 3:

- Migrating LEAP to EAP-FAST Support

Feature Descriptions

WEP
WEP is a security protocol for WLANs defined in the 802.11b standard. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one endpoint to another. However, it has been found that WEP is not as secure as once believed.

IEEE 802.11 and IEEE 802.1X
IEEE 802.11 provides standards-based interoperability between WLAN client devices and WLAN infrastructure products such as access points. The 802.1X standard is designed to enhance the security of WLANs that follow the IEEE 802.11 standard. 802.1X provides an authentication framework for WLANs, allowing a user to be authenticated by a central authority. The actual algorithm that is used to determine whether a user is authentic is left open; multiple algorithms are possible.

Wi-Fi Compliance
Wi-Fi is another name for IEEE 802.11 that was introduced by the Wi-Fi Alliance. Products certified as "Wi-Fi compliant" by the alliance are interoperable with each other, even if they are from different manufacturers.

WHQL
WHQL is a Microsoft facility that tests and certifies third-party hardware and driver products for compatibility with Windows operating systems. Products that meet the compatibility requirements are allowed to display Windows logos on product packaging, advertising, collateral, and other marketing materials, indicating that the product has met the standards of Microsoft and that the product works with Windows operating systems. Once a product has received the WHQL logo, it is listed on the Microsoft Hardware Compatibility List.

WPA Compliance
WPA is a Wi-Fi Alliance standard that was designed to improve upon the security features of WEP. The technology works with existing Wi-Fi products that have been enabled with WEP (software upgrades to existing hardware, for example), but the technology includes two improvements over WEP:

- 802.1X for user authentication
- Improved data encryption through TKIP, which scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys have not been tampered with

LEAP
LEAP is an 802.1X authentication type that uses a user name and static login password, usually a Windows login password.

Cisco Pre-standard TKIP
Provides a pre-standard implementation of TKIP, with a hashing algorithm and an integrity-checking feature, that was introduced prior to WPA TKIP for existing Cisco customers to resolve vulnerabilities with WEP.

PEAP with EAP-GTC Support
PEAP is an 802.1X authentication type where authentication follows this sequence of events:

- Client uses a digital certificate to authenticate authentication server
- Client and server create an encrypted SSL/TLS tunnel
- Server authenticates client through EAP messages in the tunnel

With PEAP-GTC, client authentication occurs via EAP-GTC, which provides support for several types of passwords, including one-time passwords, to user databases such as Active Directory, Novell Directory Services, and Lightweight Directory Access Protocol (LDAP).

Standard (WPA) TKIP with LEAP and PEAP-GTC
This ensures that WPA TKIP is tested with two popular 802.1X types-LEAP and PEAP-GTC.

Interoperability with Access Points that Support Multiple SSIDs and VLANs
This feature supports VLAN trunking for WLANs by mapping SSIDs to standard VLANs. It provides the ability to segregate user classes on each access point for purposes such as different security types, different user classes, and different application types per wireless VLAN.

Pre-standard eDCF
Pre-standard eDCF provides an early implementation of IEEE 802.11 TGe, which provides QoS across WLANs as described below:

- QoS refers to the capability of a network to provide better service to selected network traffic over various network technologies. QoS technologies provide the building blocks for business multimedia and voice applications used in campus, WAN, and service provider networks. QoS allows network managers to establish service-level agreements

(SLAs) with their network users.

- QoS enables network resources to be shared more efficiently and expedites the handling of mission-critical applications. It manages time-sensitive multimedia and voice application traffic to help ensure that this traffic receives higher priority, greater bandwidth, and less delay than best-effort data traffic. With QoS, network managers can manage bandwidth more efficiently across LANs and WANs.

QoS provides enhanced and predictable network service by:

- Supporting dedicated bandwidth for critical users and applications
- Controlling jitter and latency (required by real-time traffic)
- Managing and minimizing network congestion
- Shaping network traffic to smooth the traffic flow
- Setting network traffic priorities

Access Point Assisted Roaming
Using the information from the access point within the Inter-Access Point Protocol (IAPP), the time to roam is greatly reduced for the client devices. Access point assisted roaming decreases roaming times, increases the predictability of client roams between access points, and increases reliability and robustness of WLAN networks.

Fast 802.1X Reauthentication
Fast 802.1X reauthentication provides a mechanism that can perform secure roaming while maintaining sub-second roaming times, and that can support voice, video, and data transmissions across a WLAN infrastructure to devices that are roaming within a subnet. This increases the predictability and performance of WLAN networks while secure encryption and authentication are maintained.

Radio Environment Reporting
The radio environment reporting feature allows the client device to participate in the Cisco Structured Wireless-Aware Network (SWAN) framework. Clients are enabled to provide specific radio environment information in a device's area of operation and report this information back to the network. This reporting will describe and report, in real time, any wireless anomalies affecting the surrounding client air space. Environment reporting allows mobile devices to detect and report any potential problems such as interference, rogue access points, and unauthenticated devices in the surrounding air space. This increases the overall visibility, manageability, and performance of the wireless network.

Access Point Specified Maximum Transmit Power
Controlling the power output of clients from Cisco Aironet access points increases the reliability and performance of the wireless network. With the ability to identify the number of associated clients, cell sizes, and adjacent access point radio signals, the access points can determine the optimum power transmit power required for the clients. The ability to dynamically set client output power during the association process will increase the overall performance of the wireless network and improve WLAN device battery life.

Cisco Compatible Version Control
Version control allows the Cisco Aironet access point and infrastructure to determine what versions of Cisco Compatible Extensions program devices are communicating on the wireless network, and allows the clients to use the correct features and attributes in a mixed environment. This allows Version 1 and Version 2 devices to integrate and operate properly in a mixed environment, without any device or network management requirements.

Business Benefits

The Cisco Compatible Extensions program for WLAN devices provides assurance of compatibility with more than 130 products and devices, coupled with the innovative features of Cisco Aironet WLAN products, delivering the confidence IT managers need to deploy WLANs in their networks today. The Cisco Compatible Extensions program for WLAN devices:

- Provides tested compatibility with licensed Cisco infrastructure innovations, with more than 39 specific features to date
- Enables widespread availability of wireless devices that use Cisco Aironet infrastructure products
- Accelerates the availability of innovative features while maintaining interoperability through wireless standards
- Promotes investment protection of client devices by maintaining compatibility with industry standards and innovative Cisco infrastructure features

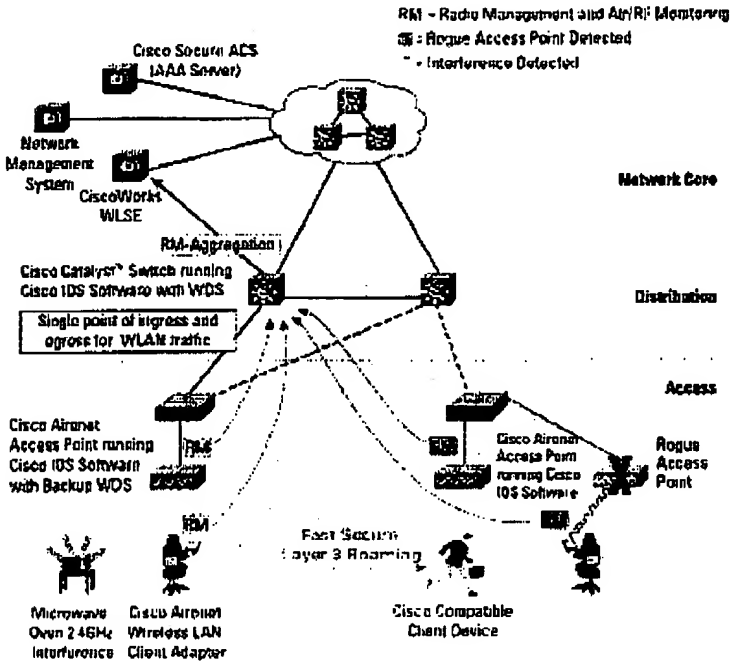
Architecture

Cisco Compatible Extensions program clients play an important part in Cisco SWAN. Many of the features available in the Cisco SWAN framework provide exclusive benefits to Cisco Compatible clients. These features enable the clients to collect and report information about the RF environment. Some of the areas of client participation in SWAN include:

- Rogue access point detection and location
- Air/RF scanning and monitoring
- Interference detection to isolate and locate network interference
- Simplified WLAN deployment processes with assisted site surveys
- Streamlined WLAN management and operations support
- High availability with self-healing WLANs

Figure 2 provides a detailed overview of the Cisco SWAN architecture and highlights the interaction of Cisco Compatible Extensions program devices in the participation and collection of important wireless information used to increase performance, scalability, security, and management of the wireless network.

Figure 2 - Cisco SWAN Architecture with Cisco Compatible Extensions Devices



Supporting Products and Partners

Review the listing of all the products that are approved in the Cisco Compatible Extensions program.

Why Cisco

With the Cisco Compatible Extensions program, Cisco is able to deliver next-generation WLAN features today. Some of these features will be adopted by the standards bodies, and Cisco will provide these as they are ratified.

Cisco Aironet infrastructure products deliver enhanced client features and services that are required for the next-generation WLAN networks that are deployed today. Through partnerships with leading WLAN device vendors, availability of Cisco Compatible Extensions program devices can be assured-with more than 130 wireless devices certified and available today (and more being added). No other WLAN vendor has the ability to take advantage of tomorrow's enhancements today providing the ability to confidently deploy robust, scalable, secure, and manageable solutions.

For More Information

For more information about the Cisco Compatible Extensions program, contact your local account representative or visit:

www.cisco.com/go/ciscocompatible/wireless